EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 01098032
PUBLICATION DATE : 17-04-89

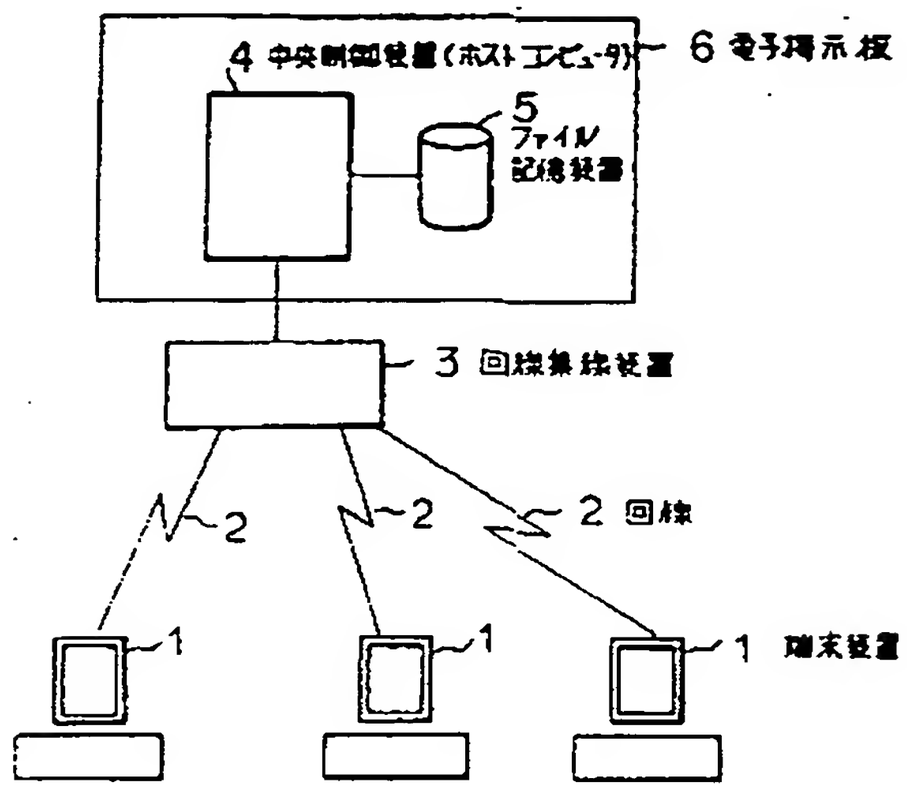
APPLICATION DATE : 09-10-87
APPLICATION NUMBER : 62255808

APPLICANT : NIPPON TELEGR & TELEPH CORP <NTT>;

INVENTOR : MORITA HIKARI;

INT.CL. : G06F 11/00 G09C 1/00

TITLE : PROTECTION METHOD FOR CODING SHARED INFORMATION



ABSTRACT : PURPOSE: To protect the shared information using ciphers in an electronic billboard system by securing such a constitution where a transmitter of information informs the presence of information to many and unspecified participators via a title and at the same time delivers a key of the ciphered text to a selected person of the remote side by means of an electronic mail, etc.

CONSTITUTION: A user's terminal equipment 1 containing a ciphering device is connected to a circuit line concentrator 3 via a circuit 2. The concentrator 3 is connected to a CPU 4 consisting of a host computer. The CPU 4 controls a file memory 5 which stores the documents received from many users. Then an electronic billboard 6 consists of the CPU 4 and the memory 5. An optional part of the information supplied from the equipment 1 is ciphered as necessary and sent to the memory 5 of the CPU 4 to be stored and shared. Thus the user calls the billboard 6 and can read all titles and also the subtitles. However it is impossible to decode the extracted sentences as long as they are ciphered by a transmitter. When the user request a key via an electronic mail, a telephone, etc., the transmitter delivers the key to the requester after confirmation.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1-98032

⑤1Int.Cl.⁴	識別記号	庁内整理番号
G 06 F 11/00	340	7368-5B
G 09 C 1/00		7368-5B

⑬公開　平成1年(1989)4月17日

審査請求　未請求　発明の数 1　(全3頁)

⑤4発明の名称　共有情報暗号化保護方法

⑳特　願　昭62-255808

㉒出　願　昭62(1987)10月9日

⑦2発明者　山根　道広　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

⑦2発明者　森田　光　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

⑦1出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号

⑦4代理人　弁理士　草野　卓

明　細　書

1．発明の名称

共有情報暗号化保護方法

2．特許請求の範囲

(1)　暗号装置を備えた複数の端末装置と、

これら端末装置を収容する集線装置と、

その集線装置に接続された中央制御装置と、

その中央制御装置により制御されるファイル記憶装置とから構成され、

上記端末装置から入力される情報に暗号を施して上記ファイル記憶装置に送り格納、共有化し、

他の端末装置からの情報転送要求に対して上記ファイル記憶装置内の共有情報を要求元の端末装置へ転送し、

情報要求者は情報発信者より暗号解読のための鍵を入手し、

その鍵を用いて暗号文を解読することを特徴とする共有情報暗号化保護方法。

3.　発明の詳細な説明

「産業上の利用分野」

この発明は多数の端末装置から共同で利用可能なパソコンネットワーク、ＬＡＮ（ローカルエリアネットワーク）などにおいて広く利用されている電子掲示板などに投入、共有化されたデータや文などの情報を保護する共有情報暗号化保護方法に関する。

「従来の技術」

電子掲示板等に於いて、共有化されたデータや文の保護には、従来以下に述べるようなパスワードを用いたアクセス制御方法が用いられている。

第3図に電子掲示板におけるパスワードを用いた階層型のアクセス制御の概念図を示す。階層型のアクセス制御では、掲示板に掲示される文章は表題、副表題、本文の三層に分割され、それぞれに個別のパスワードが設定される。

掲示板の利用者が掲示板を閲覧するには第一のパスワードを端末より電子掲示板システムに投入する。その結果、掲示されている全ての文章の表題を読むことが出来る。一般に表題は文字数が限られているため書かれている内容を的確に把握す

るには不足である。そのため、第二のパスワードは副表題を読み出すために用いられる。利用者が副表題までを読んで、さらに詳しい情報を得るためには第三のパスワードが必要である。

このようにして、パスワードにより多くの利用者の知ることの出来る情報の範囲（階層）を制御する事が出来る。しかし、このパスワードを用いたアクセス制御方法では保護階層毎の全てのパスワードを持つ人であれば誰でも全ての文章を読むことが出来る。すなわち、電子掲示板を制御しているコンピュータがパスワードをチェックし許可すれば、発信者の望まない相手にも本文が読まれてしまう。パスワードを用いたアクセス制御方法を採用した電子掲示板では、広く広報する事は出来るが、情報発信者が情報を伝えたい相手を選別する事が出来ない。

この様なパスワードを用いた階層型のアクセス制御の欠点を補う方法として、以下のようなパスワードの設定方法が考えられる。

表題、副表題のアクセス制御は階層型のパスワードとし、本文へのアクセス制御を行うパスワードは情報毎に設定する。この様にすれば、情報発信者が情報を伝えたい相手を選別する事が出来る。

しかし、パスワードを用いたアクセス制御では、予めパスワードとして設定されたデータと、アクセス時に投入されたデータとを比較することにより行う。そのため、あたかも正しいパスワードが投入されたかの様に計算機を操作したり、設定されているパスワードを盗み出すなどの方法による、共有化されたデータへの不正なアクセスを完全に防ぐことが出来ない。

以上のように、従来のパスワードを用いた共有情報を保護する方法では、情報発信者が情報を伝えたい相手を選別する事が出来ない、またパスワードによるアクセス制御を回避するような不正なアクセスから共有情報を十分保護することが出来ないなどの欠点があった。

この発明の目的は、パソコンネットワークやＬＡＮなどの電子掲示板システムにおいて、情報発信者が情報の存在を不特定多数の参加者に伝えると同時に、情報発信者が情報を伝えたい相手を選別する事が出来、不正な手段により共有情報が読みだされても利用されることを防止することが可能な、暗号装置を用いた共有情報暗号化保護方法を提供することにある。

「問題点を解決するための手段」

この発明によれば、各端末装置には暗号装置が設けられ、これら端末装置は集線装置を介して中央制御装置に接続され、その中央制御装置に制御されるファイル記憶装置が設けられ、端末装置から入力される情報に暗号を施してファイル記憶装置に送り格納、共有化し、他の端末装置からの情報転送要求に対してファイル記憶装置内の共有情報を要求元の端末装置へ転送し、情報要求者は情報発信者より暗号解読のための鍵を入手し、その鍵を用いて暗号文を解読する。

このようにこの発明では情報発信者は情報を伝えたくない相手か否かを確認して情報要求者へ鍵を渡すことができ、情報発信者は情報を伝えたい相手を選別することができ、かつファイル記憶装置内の情報は暗号化されているためハッカーなどによる共有情報の不当な読み出しを防ぐことができる。

「実施例」

第１図はこの発明の実施例に用いられる電子掲示板システム例を示す。暗号装置を備えた利用者の端末装置１は回線２を通じて集線装置３に接続され、集線装置３はホストコンピュータよりなる中央制御装置４に接続され、中央制御装置４により、多数の利用者からの文書を蓄積するファイル記憶装置５が制御される。中央制御装置４及びファイル記憶装置５は電子掲示板６を構成している。

端末装置１から入力される情報の任意の部分に必要に応じて暗号を施して中央制御装置４のファイル記憶装置５に送り格納、共有化される。つまり情報発信者は、第２図に示す様に発信文書に暗号を施す。表題、副表題だけで十分内容が伝えられると思われる場合は本文全体を暗号化し、表題、副表題だけでは十分内容が伝えられないと思われる場合やアイディアの中心部分は隠しておきたい

場合などは本文を部分的に暗号化し電子掲示板に投入する。勿論、利用者を選別する必要のない場合は、全文を暗号化せずに投入する。

利用者が端末装置1より電子掲示板6を呼び出すと、まず投入されている全ての表題が閲覧出来る。それらの表題のよりさらに詳しい情報を得たい場合には、表題をもとに副表題さらには全文を取り出すことが出来る。しかし、発信者により暗号が施されている場合は取り出した文を解読する事は不可能である。暗号文を解読したい場合には、暗号化された文をそのまま端末装置1内に格納し、電子メールにより発信者に暗号解読のための鍵を要求する。暗号鍵の請求を受けた発信者は電子メールにより請求者を確認し鍵を手渡す。鍵の授受は必ずしも電子メールである必要はなく、電話等他の通信手段でも良い。

但し、暗号によるデータの安全性は、鍵の安全性と相対的であるので、鍵の授受には十分注意して行う必要がある。

「発明の効果」

この発明によれば、不特定多数のユーザが利用するパソコンネットワークやＬＡＮなどの電子掲示板システムに於て、情報発信者が情報の存在を不特定多数の参加者に伝えると同時に、情報発信者が情報を伝えたい相手を選別する事が出来、不正な手段により共有情報が読みだされても利用されることを防ぐことの可能な、暗号装置を用いた共有情報暗号化保護方式を提供することにある。

更に、ユーザ・センタ間において転送されるデータは暗号化されているめ、回線途上に於ける盗聴等に対してもデータを保護することが出来る。

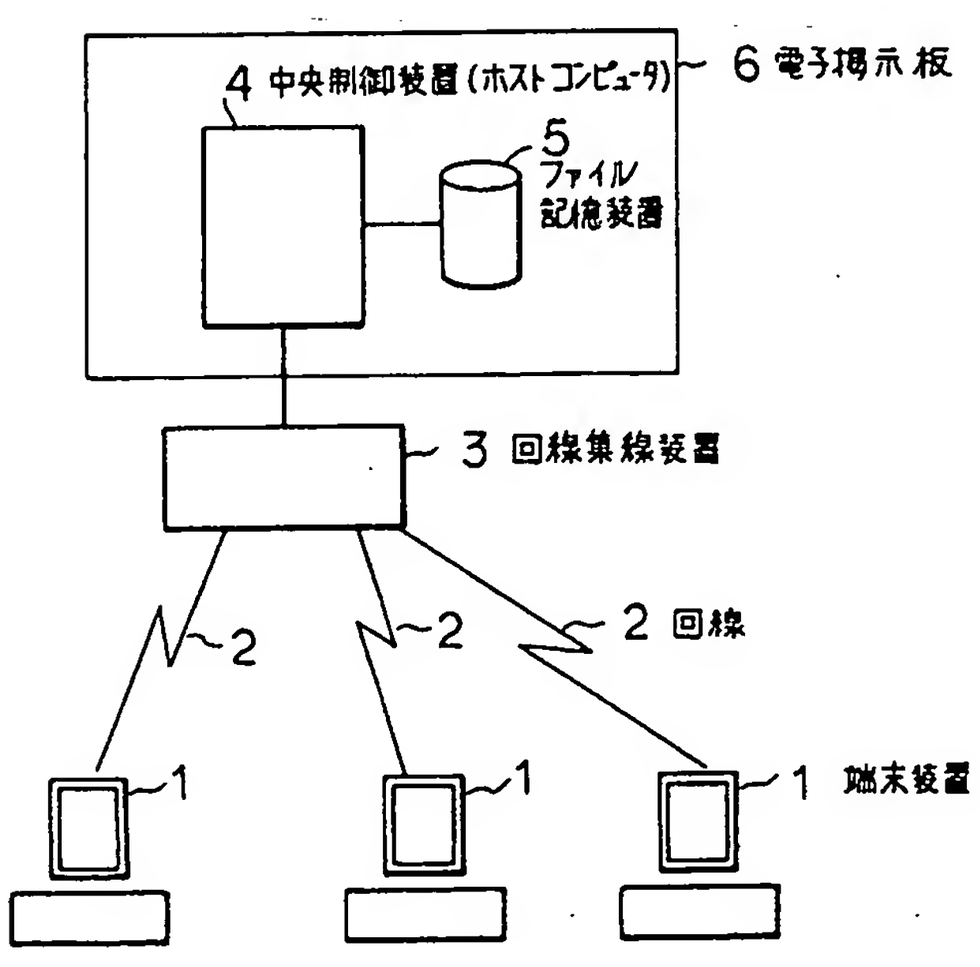
4. 図面の簡単な説明

第1図は電子掲示板システムの構成例を示すブロック図、第2図は発信文書に暗号を施した例を示す図、第3図は電子掲示板におけるパスワードを用いた階層形アクセス制御の概念を示す図である。

特許出願人：日本電信電話株式会社

代　理　人：草　野　　卓

第　1　図



第　2　図

表題	副表題
抜け道情報	関越線島出口～東名用賀インタ

本文
関越インタを出て一番目の××××××××××
××××××××××××××××××××
××××××××××××××××××××
××××××××××××××××××××
××××××××××××××××××××
この道は早道マップにも出ていない最短時間の道です。　詳細はメール NO.3247まで。

××の部分は暗号化されている。

第　3　図